#28 10/9/02 A.W

PATENT
Attorney Docket No.: 80410.0009

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

MOSKOWITZ, Scott, et al

Appl. No.: 08/999,766

Filed: July 23, 1997

For: Steganographic Method and Device

Art Unit: 2132

Examiner: MEISLAHN, D.

Commissioner for Patents
Washington DC 20231

Sir:

RESPONSE TO OFFICE ACTION (PAPER NO. 27)

This Response and Amendment is submitted in response to the non-final Office Action dated April 5, 2002 (Paper No. 27).

REQUEST FOR EXTENSION OF TIME

Applicant respectfully requests a three (3) month extension of time to respond to the non-final Office Action of April 5, 2002, extending the period for response from July 5, 2002 to October 5, 2002. A check in the amount of $460.00 is attached to cover the extension fee. It is believed that no other fees are required to ensure entry and consideration of this response. However, if any fees are required with the filing of this response, Applicants respectfully request that any such fees be charged to Deposit Account No. 50-1129.

RESPONSE TO OFFICE ACTION

Definition of Stega-Cipher

With all due respect, Applicant traverses Examiner's assertion in paragraph 3 that "applicant's definition of a stega-cipher is not material to the claims." The term "stega-cipher" is a claim term, and therefore, "stega-cipher" is *ipso facto* material to the claims. Moreover, it was

Supervisory Examiner Hayes who required Applicant to set forth a definition for the term so that the claims could be discussed in view of the definition.

For convenience, Applicant's definition of stega-cipher is repeated below:

> A stega-cipher (a.k.a. a steganographic cipher) is an algorithm or combination of algorithms that performs two functions: (1) a steganographic function to determine where in the carrier signal, data (such as message data or watermark data) can be hidden "in plain view"; and (2) a cipher function that makes use of potential data location information, a random or pseudo random seed, and the message data to generate a key that randomly maps the message data into the carrier signal. The use of the phrase "in plain view" does not limit the claimed invention to visual applications.

Support for the Definition of Stega-Cipher

In the response dated December 11, 2001, Applicant submitted extensive support for the proposed definition of stega-cipher. Applicant submits that each aspect of the cipher function is supported by the specification. In particular, and without limitation, Applicant submits that sample embodiments support the cipher function as described in the definition of stega-cipher, namely, pages 18, line 5 through page 24, line 9 (with only the most relevant portions being produced below) (emphasis added):

> III. Example Embodiment of Encoding and Decoding
>
> A modification to standard steganographic technique is applied in the frequency domain described above, in order to encode additional information into the audio signal.
>
> In a scheme adapted from cryptographic techniques, 2 keys are used in the actual encode and decode process. For the purposes of this invention the keys are referred to as masks. One mask, the primary, is applied to the frequency axis of FFT results, the other mask is applied to the time axis (this will be called the convolution mask). The number of bits comprising the primary mask are equal to the sample window size in samples (or the number of frequency bands computed by the FFT process), 128 in this discussion. The number of bits in the convolution mask are entirely arbitrary. This implementation will assume a time mask of 1024 bits. Generally the larger the key, the more difficult it is to guess.
>
> Prior to encoding, the primary and convolution masks described above are generated by a cryptographically secure random generation process. It is possible to use a block cipher like DES in combination with a sufficiently pseudo-random seed value to emulate a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in decoding, should that step become necessary.
>
> ...

Starting with the lowest frequency band, the encoder proceeds through each band to the highest, visiting each of the 128 frequency bands in order. At each band value, the encoder takes the bit of the primary mask corresponding to the frequency band in question, the bit of the convolution mask corresponding to the window in question, and passes these values into a boolean function. This function is designed so that it has a near perfectly random output distribution. It will return true for approximately 50% of its input permutations, and false for the other 50%. The value returned for a given set of inputs is fixed, however, so that it will always return the same value given the same set of inputs.

If the function returns true, the current frequency band in the current window is used in the encoding process, and represents a valid piece of the additional information encoded in the signal. If the function returns false, this cell, as the frequency band in a given window is called, is ignored in the process. In this manner it is made extremely difficult to extract the encoded information from the signal without the use of the exact masks used in the encoding process. This is one place in which the stega-cipher process departs from traditional steganographic implementations, which offer a trivial decode opportunity if one knows the information is present. While this increases the information storage capacity of the carrier signal, it makes decoding trivial, and further degrades the signal. Note that it is possible and desirable to modify the boolean cell flag function so that it returns true <50% of the time. In general, the fewer cells actually used in the encode, the more difficult they will be to find and the less degradation of content will be caused, provided the function is designed correctly. There is an obvious tradeoff in storage capacity for this increased security and quality.

The encoder proceeds in this manner until a complete copy of the additional information has been encoded in the carrier signal. It will be desirable to have the encoder encode multiple copies of the additional information continuously over the duration of the carrier signal, so that a complete instance of this information may be recovered from a smaller segment of a larger signal which has been split into discontinuous pieces or otherwise edited. It is therefore desirable to minimize the size of the information to be encoded using both compact design and pre-encoding compression, thus maximizing redundant encoding, and recoverability from smaller segments. In a practical implementation of this system it is

The encoder will also prepare the package of additional information so that it contains an easily recognizable start of message delimiter, which can be unique to each encoding and stored along with the keys, to serve as a synchronization signal to a decoder. The detection of this delimiter in a decoding window signifies that the decoder can be reasonably sure it is aligned to the sample stream correctly and can proceed in a methodic window by window manner. These delimiters will require a number of bits which minimizes the probability that this bit sequence is not reproduced in a random occurrence, causing an accidental misalignment of the decoder. A minimum of 256 bits is recommended. In the current implementation 1024 bits representing a start of message delimiter are used. If each sample is random, then each bit has a 50% probably of matching the delimiter and the conditional probability of a random

match would be $1/2^{1024}$. In practice, the samples are probably somewhat less than random, increasing the probability of a match somewhat.

In this embodiment, it is significant that the number of bits in the primary mask equals the number of elements in each sample window. This permits the stega-cipher to view each of the elements of the sample window as a potential location to encode information. Note that the actual content of the primary mask and the actual content of the convolution mask represent random or pseudorandom data, which, in effect, serve as the random or pseudo random seed. Finally, the message data itself is part of the key in that it is placed within the carrier data.

Applicant also submits that the claims as they existed at the time of filing the application also support the definition of stega-cipher. See, for example, original claim 3, pages 39-41 (which discloses how the processor loops through each sample window and utilizes a bit of a random 128 bit primary mask and a bit of a random 1024 bit convolution mask to calculate an offset into a stega-cipher map truth table, and encodes a bit of the message data into the sample when the map function is true).

Applicant also submits that the pseudo-code submitted in the appendix to the application (pages 54-64) also support the definition of stega-cipher (disclosing how the processor loops through each sample window and utilizes a bit of a random 128 bit primary mask and a bit of a random 1024 bit convolution mask to calculate an offset into a stega-cipher map function, and encodes a bit of the message data into the sample when the map function is true).

Initialization of Stega-Cipher

Previously, Examiner requested Application to confirm that the stega-cipher of the present invention uniquely marks each and every copy of data that is made using the invention. In other words, if you run the stega-cipher on the same carrier data, using the same message data, and the same random or pseudo random key, the output will be different each time the stega-cipher is run. (See Specification, Page 9, lines 18-20, "The invention uniquely identifies every copy of multimedia content made using the invention..."). Applicant confirmed this per Examiner's request.

Examiner expresses skepticism, and then engages in what Examiner acknowledges to be "conjecture" regarding random function and the use of a "seed" to initialize an "internal state." Moreover, Examiner's arguments seem internally inconsistent in that the argument states that the

outputs of the stega-cipher could be different "but only if *f* is a random function." Examiner then asserts that *f* is not a random function, and yet acknowledges the use of random variables. Applicant requests clarification. It may be that Examiner is trying to make a helpful suggestion, but any suggestion is lost in the inconsistencies. Applicant, however, again confirms that the stega-cipher of the present invention uniquely marks each and every copy of data that is made using the invention.

Regardless, Applicant submits that Examiner's analysis overlooks one simple explanation as to how the stega-cipher creates a unique output even when using the same exact input. The stega-cipher creates a unique output, in part, because the starting point of the encoding is random.

Rejections under 35 U.S.C. § 112

Examiner asserts that for reasons "there is no teaching of using the watermark or potential data locations to form the key." Applicant submits that as discussed above, there is support for the proposed definition of stega-cipher.

Multiplicity of Rejections

Applicant submits that the rejections in this case are multiplicative, and have significantly and unreasonably increased the cost of prosecution in this case. Exhibit A attached hereto indicates that each and every pending claim has been rejected twice using different references and/or combinations of references. Such duplicative rejections have forced application to incur substantial costs in responding to this office action.

Applicant also submits further that multiplicative rejections are contrary to the guidelines set forth in the Manual of Patent Examination and Procedure:

> In selecting the references to be cited, the examiner should carefully compare the references with one another and with the applicant's disclosure to avoid the citation of an unnecessary number. The examiner is not called upon to cite all references that may be available, but only the "best." (37 CFR 1.104(c).) **Multiplying references, any one of which is as good as, but no better than, the others, adds to the burden and cost of prosecution and should therefore be avoided**. ...
>
> **The best reference should always be the one used**. Sometimes the best reference will have a publication date less than a year prior to the application filing date, hence it will be open to being overcome under 37 CFR 1.131. In these

> cases, if a second reference exists which cannot be so overcome and which, though inferior, is an adequate basis for rejection, the claims should be additionally rejected thereon.

MPEP § 904.3

The examiner's rejections under 102 demonstrate that the examiner's "best reference" is the published patent application EPO 0 581 317 A2 ("Powell"). This deduction is based upon the Examiner's use of Powell in making the 102 rejections. The Examiner uses two references to sets forth two sets of 102 rejections, namely, one set based on Powell, and another based on an article entitle "Techniques for Data Hiding" ("Bender"). In particular Bender, is used to reject claims 25, 27-29, 31-33, 35, 62 and 63. The Examiner, however, uses Powell to reject not only the same claims as Bender, but also six (6) additional claims (collectively, rejecting claims 25-33, 35-39, 62 and 63). In other words, the Examiner considered Powell sufficient by itself to reject claims 26, 30, and 36-39, while the Examiner had to combine Bender with another reference to reject the same claims under 103. Clearly, the guidelines set forth in MPEP 904.3 would indicate that Powell should be used in lieu of Bender, which would have cut in half the number of rejections made by Examiner (78 rejections could have been reduced to 39).

As a result of the duplicative rejections, Applicant is forced to address each of the arguments raised by Examiner, resulting in significantly increased costs and time in preparing this response.

Rejections under 35 U.S.C. § 102

1. § 102 Rejections based on Bender

Claims 25, 27-29, 31-33, 35, and 62 stand rejected as allegedly anticipated by Bender. (See ¶10 of the Office Action). The entirety of the examiner's support for these 102 rejections is as follows:

> In their introduction on page 164, Bender et al. distinguish between data hiding and encryption. They also state that hidden data should be "invisible" or inaudible", which meets the limitations of claims 62 and 63. In the first paragraph of the next page, they say that watermarks are one type of data often inserted into files. In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined. In section 1.2 Bender is mentioned as encrypting the embedded data. A reading of the section cited as support for the

> amendment of 17 January 2001 seems to say that this feature is not inherent to a stega-cipher, but is not quire entirely clear.

(Office Action of April 5, 2002, p. 5).

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, inter alia, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal...." Independent Claim 29 contains similar language. The 102 rejection based on Bender is improper for at least the reason that Bender fails to disclose the use of a stega-cipher as required by the rejected claims.

The "key" allegedly disclosed in Bender (see Bender, p. 171) is not the same as a stega-cipher used to steganographically encode independent data into a carrier signal within the meaning of the present claims. In fact, there are several differences between a stega-cipher as used in the present invention, and the alleged "key" described in Section 3.4 of Bender. As stated in Bender:

> In [Direct Sequence or "DS"], a "key" is needed to encode the information and the same "key" is needed to decode it. The key is pseudo-random noise that ideally has flat frequency response over the frequency range, i.e., white noise. The key is applied to the coded information to modulate the sequence into a spread spectrum sequence.

(Bender at 171). With Bender, the same "key" is used for both encoding and decoding. The stega-cipher being used in the present invention is not so limited. With the present invention, the encode and decode keys may be symmetric or asymmetric depending on the application. Bender's "key" is not ciphered in any manner, but is simply a pseudo-random sequences based on the white noise inherent to the signal. Moreover, even for symmetric applications of the present invention where the encode key and decode key may be the same, the actual mapped locations may be different for each copy encoded of a given carrier signal.

Spread spectrum "is designed to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible." (Bender at 171). Spread spectrum spreads the encrypted data across the spectrum by using a "key" that has "maximum randomness and flat frequency spectrum." (Bender at 172). Bender's "chip" or "key" "is a pseudo-random sequence modulated at a known rate." (Bender at 171). This is very different than the stega-cipher of the present invention. A stega-cipher is not a pseudo-random sequence modulated at a known rate.

As disclosed in the specification the "stega-cipher" borrows from both steganography and encryption:

> The invention draws on techniques from two fields, cryptography, the art of scrambling messages so that only the intended recipient may read them, and steganography, a term applied to various techniques for obscuring messages so that only the intended parties to a message even know that a message has been sent, thus it is termed herein as a stega-cipher. The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content. The message itself is encrypted which serves to further protect the message, verify the validity of the message, and redistribute the information in a random manner so that anyone attempting to locate the message without the keys cannot rely on pre-supposed knowledge of the message contents as a help in locating it.

(Patent Application, p. 7, lines 13-25). Basically, the steganographic portion of the stega-cipher seeks to identify locations within the carrier signal where information may be stored, but it is the cipher portion of the stega-cipher determines which of those identified locations will be actually used. If all of the locations are used, then it will be easier for others to remove the encoded information, because you can run similar algorithms to identify the candidate locations. The cipher portion uses a mask to encode the independent data into those identified areas, such that not all of the available locations are used. Hence, a hacker will have to wipe out all or almost all of the identified areas to remove the watermark (or simply guess at the potential locations), which generally will degrade the quality of the carrier signal significantly. Bender's key has no such masking. Accordingly, a "stega-cipher" is not the same as Bender's "chip."

Moreover, there are differences in how the present invention and how Bender's system detect and read the respective encoded information. Bender's system requires that the "key stream for encoding is known by the receiver" and, in addition, the "following parameters are known by the receiver: chip rate, data rate, carrier frequency, and the data interval." (Bender at 172). This is a lot of information that must be known to decode the encoded data. In the present invention, one only needs a stega-cipher, and more particularly, the key associated with the stega-cipher, to decode.

A stega-cipher, unlike spread spectrum, seeks to maximize the imperceptibility by limiting the number of bits being encoded. This is antithetical to spread spectrum's adding white noise because to encode data as flat spectrum noise requires significantly more data to be

encoded. This point is evidenced by the differences between the seeding of Bender's "chip" and the seeding of a stega-cipher of the present invention. Bender's "chip" is a pseudo-random sequence modulated at a known rate." (Bender at 171). Each bit in Bender's chip is encoded into the signal, whereas with a stega-cipher, only select bits are encoded. Moreover, with a stega-cipher, it is possible that each encoding yields a completely different result as to where watermarks are located. This is a very different result from that contemplated by Bender.

Because Bender fails to disclose a "stega-cipher" as required by claims 25 and 29, the 102 rejection of 25 and 29 must be withdrawn. Moreover, for the same reasons that claims 25 and 29 are patentable over Bender, the claims that depend from claims 25 and 29 are also patentable. Applicant requests the Examiner to withdraw the § 102 rejections based on Bender.

2. § 102 Rejections based on Powell

Claims 25-33, 35-39, 62 and 63 stand rejected as allegedly anticipated by Powell. (See ¶11 of the Office Action). The entirety of the examiner's support for these 102 rejections is as follows: "See page 4, lines 4 and 40-42." (Office Action of April 5, 2002, p. 5).

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, inter alia, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal ...." Independent Claim 29 contains similar language. The 102 rejection based on Powell is improper for at least the reason that Powell fails to disclose the use of a stega-cipher as required by the rejected claims.

Powell does not disclose the use of a stega-cipher as claimed by the present invention for at least the following reasons: 1) Powell does not disclose the use of a cipher; 2) Powell does not disclose the use of a key; 3) Powell does not embed independent data into a carrier signal; and 4) Powell does not disclose a relationship between the message, signal and key or cipher. In particular, Powell does not disclose the use of a cipher function that makes use of potential data location information, a random or pseudo random seed, and the message data to generate a key that maps the message data into the carrier signal. Powell does suggest that a computer "can be programmed to choose signature points randomly or accordingly to a predetermined pattern" (Powell, page. 4 lines, 40-42), but this is not the same as using a cipher to identify which extrema will be used. Moreover, Powell does not utilize any key—which is why the "image signature" can only be retrieved through the use of the original, unaltered image (Powell, page 5, line 51-page 6, line 9). The use of keys to encode also permits the use of keys to decode, resulting in a

significant practical difference between Powell's teachings and those of the present invention. Since an object of the present invention is to protect the original data, it is undesirable (and, indeed, very risky) to circulate unwatermarked copies of the original data for decode purposes. Circulation of the decode key, rather than the original data, helps to protect the original data from the risk of unauthorized and untraceable copying. For this additional reason, Applicant's invention teaches away from Powell.

Finally, Powell does not embed independent data into the digital image as required by the claimed invention. In Powell, the pixel value (which is a luminance value) is adjusted a small positive or negative amount (preferably 2% to 10% of the initial pixel value), whereby the difference is indicative of a "1" or a "0". (Powell, page 4 lines 42-48). Hence, Powell teaches replacing a pixel value with a new value that is dependent upon the initial value (adjusted upwards or downwards 2-10%) of the pixel. If the value were not dependent upon the initial value, the embedding would not be inconspicuous. Therefore, for at least this additional reason, Powell is distinguishable.

Rejections under 35 U.S.C. § 103

1. The Combination Of References Fail To Disclose All Of The Claimed Limitations.

In order to establish a prima facie case of obviousness, at least two criteria must be met. First, there must be some motivation or suggestion to make the proposed combination or modification of the references. Further, "the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's disclosure." MPEP 2142, discussing In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). In addition, the combined references must teach or suggest all claim limitations.

As discussed below, there is no sufficient teaching or suggestion for combining the references as Examiner has combined them. Further, the references, when combined, fail to yield the claimed inventions. For at least these reasons, the 103 rejections must be withdrawn.

a) None of the References Disclose the "Stega-cipher" Limitation

The Examiner has failed to establish a prima facie case of obviousness for each and every one of the 103 rejections because the cited references, either alone or in combination, failed to

disclose all of the claimed elements. All of the Examiner's 103 rejections are based in whole or in part upon Bender or Powell. As discussed above in connection with the 102 rejections, neither Bender nor Powell disclose the use of a "stega-cipher" as required by the independent claims in the application (namely, claims 25 & 29). In fact, noticeably absent from the Examiner's 103 rejections is any discussion whatsoever of the claimed invention's use of a stega-cipher. For at least this reason, the Examiner has failed to establish a prima facie case of obviousness for all claims that depend from Claims 25 and 29. MPEP 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.") (quoting In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)). Thus, the 103 rejections of 26-28 and 30-63 cannot stand.

b) The Examiner Appears To Have Misread Powell

In the Office Action, the Examiner acknowledges the distinction between steganography from encryption, (Office Action, p. 5), but the Examiner then appears to overlook the distinctions. The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a message into the underlying data without changing its perceptible characteristics (i.e., "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

In particular, the Examiner's comments regarding Powell and certain other references suggest that the Examiner has not appreciated the distinction between steganography and encryption. For example, Examiner states several times without any detailed explanation that Powell teaches "encrypting digital watermarks into information with a key." (See ¶¶ 13, 14, 15, 16 and 17 of the Office Action). This assertion is inaccurate. It may be fair to characterize Powell to teach encoding "signatures"[1] into a carrier signal (*see, e.g.*, Powell, Abstract, which states "A method and system for embedding signatures within visual images"), but Powell does not teach "encrypting watermarks into information"—much less "encrypting watermarks into information with a key." Because the Examiner's phraseology is also inconsistent with the language of Powell, it is not entirely clear how the Examiner is construing Powell, especially

[1] Please note that the "signatures" described in Powell are not cryptographic signatures within the meaning of cryptography, nor are they stega-cipher type signatures within the context of Applicant's invention.

since the Examiner fails to relate the techniques taught by Powell to the step of "encrypting watermarks into information with a key."

c) The Combination of Powell and Schneier Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 34, 40-43, and 46-48 are unpatentable over Powell in view of Schneier[2], and that claims 44, 45 and 49 are unpatentable over Powell and Schneier in view of Cox.[3] (See ¶¶13 and 14 of the Office Action).

The entirety of the Examiner's arguments that claims 34, 40-43, and 46-48 are unpatentable over Powell in view of Schneier is as follows:

> Powell et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.
>
> Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted into the encryption of block data. The key breakdown and the subsequent permutation correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of [Applicants'] claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious . . . to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.
>
> Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

(Office Action, pp. 5-6).

DES is an encryption standard; DES is not the same as steganographic ciphering. DES processes data without regard to the perceptibility of the data, and so, the end result is an encrypted data output that looks nothing like the input. DES does not involve hiding a watermark into independent data, but rather taking the independent data and modifying it to the point that it no longer looks resembles its initial appearance. Thus, there is no "mask set" in a DES cipher. Contrary to the Examiner's assertion, the key breakdown and permutations are

---

[2] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (1994)

[3] Cox et al., "Secure Spread Spectrum Watermarking for Multimedia"

simply data, and bear little relationship, if any, to the mask set claimed in the present application. Accordingly, Applicants traverse the Examiner's assertion that the "key breakdown and subsequent permutations correspond to applicant's mask set." *Id.*

As discussed above, Powell does not teach "encrypting digital watermarks into information with a key." Even if one were to apply DES to the teachings of Powell,[4] it would not yield the claimed invention. Applying DES to Powell would logically result in an encrypted image that clearly is not the same as the claimed invention of using a stega-cipher to steganographically encode a watermark into a carrier signal. Moreover, it would appear that encrypting the image is contrary to the teachings of Powell, which states that signature points should be encoded "very inconspicuously." *See, e.g.,* Powell, p. 4, line 4.

The Examiner has simply failed to establish a prima facie case of obviousness. Moreover, The conclusion that the Examiner reaches, namely, "it would have been obvious ... to use masks to protect data" does not appear to relate to the claimed invention. The claimed invention requires the use of a stega-cipher to steganographically encode a watermark into a carrier signal. For the simple reason that combining Powell with DES would result in an encrypted image, it is clear that the result is not a steganographically-encoded watermark, as required by each of the rejected claims. This practical distinction confirms that the combination cannot yield the claimed invention. Moreover, the combination does not utilize a mask set as required by claims 40-51. For at least these independent reasons, Applicant requests the Examiner to withdraw the rejections based on the combination of Powell and Schneier.

d) The Combination of Powell and Barton Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 52-57 are unpatentable over Powell in view of Barton.[5] (See ¶¶16 and 17 of the Office Action).

With respect to claims 52-54, examiner asserts:

---

[4] After mentioning Powell in the opening premise, the Examiner does not refer to Powell again in paragraph 13 of the Office Action. It may be that the reference to "key-encrypted watermark data of Schneier" was intended to be a reference to Powell, but for the same reasons discussed in the main text, the result does not change the fact that the combination does not yield the claimed invention.

[5] U.S. Patent No. 5,912,972.

> Powell et al. teach encrypting digital watermarks into information. They do not say that the watermarks are unique. In lines 20-33 of column 4, Barton teaches including sequence data with authentication data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

(Office Action, pp. 7-8).

As discussed above, Powell does not teach "encrypting digital watermarks into information with a key," and furthermore, does not teach the use of a stega-cipher for steganographically encoding watermarks into a carrier signal. The addition of Barton does not cure this shortcoming. For at least this reason, the combination does not yield the claimed invention.

Claims 52-57 are also allowable for the reason that the combination of Powell and Barton fail to yield another aspect of claim 52. Claim 52 relates to "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream." Implicit in Claim 52 is that multiple watermarks exist in the same sample stream. The Examiner has not established where Powell (or Barton) teaches the use of multiple watermarks. Unless you have multiple watermarks, there is no need to consider marking them with unique data. Multiple watermarks may be governed by independent keys, which assist in creating uniqueness. Each encoding of a watermark may have a different strength level or different mapping location, or different random seed value, characteristics that are missing from the prior art.

The section of Barton cited by Examiner does not make obvious claims 52-55 for at least the additional reason that Barton fails to disclose "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream":

> The invention provides a method and apparatus for basic authentication of a digital block and for carrying additional authentication information provided by the user, i.e. meta-data, in a secure and reliable fashion. To embed authentication data into a digital block, a digital signature is formed that is a reduced representation of the digital block. The signature and additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance authentication capability. The encrypted data can be further verified using error correction coding techniques. For sequential data, such as the frames of a video

> display, a sequence numbers can also be provided as part of the meta-data to ensure that frames have not been deleted or re-ordered.

(U.S. Patent No. 5,912,972, Col. 4, lines 18-33). As understood, Barton encodes authentication information into a digital block by first making a digital signature of the digital block, adding meta-data provided by the user, and then encoding the digital signature and the meta data into the digital block. Barton further suggests that where the underlying data comprises sequential data such as video frames (for example, where the digital blocks represent video frames), the meta data being added can include frame numbers to indicate the sequence order. It would appear that the Examiner's argument has assumed that the meta-data represents a watermark (because it represents independent data provided by the user). The Examiner, however, is relying on the insertion of sequence information that directly relates to the underlying data. Thus, at best the Examiner's citation of Barton suggests that unique information about the underlying data can be added to the meta data to provide information about the underlying data. Claim 52 is directed to the unique identification of multiple watermarks that may be embedded into underlying data. Barton, at best, appears to teach the unique identification of the underlying data. The motivation for marking Barton's underlying data is based upon the purpose of the underlying data (e.g., video frames). This motivation does not suggest any need or desire to uniquely mark the data that is being embedded into the underlying data. So, even if you assume a motivation for combining Barton and Powell, you still do not have the invention of Claim 52, and therefore claim 52, and claims 53-57 that depend from claim 52, are not obvious. For at least this additional reason, the rejection must be withdrawn.

e) The Combination of Powell, Schneier and Barton Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 50-51 and 58-61 are unpatentable over Powell and Schneier in view of Barton. (See ¶15 of the Office Action). Applicant submits that these rejections must be withdrawn for the following reasons:

- Claim 50 is allowable for at least any one of the same reasons that claims 25, 40 and 41 were allowable as indicated above (note that claim 50 depends from claims 25, 40 and 41)

- Claim 51 is allowable for at least any one of the same reasons that claims 29, 46, 47, and 48 were allowable as indicated above (note that claim 51 depends from claims 29, 46, 47 and 48)

- Claims 58-61 are allowable for at least any one of the same reasons that claim 29 was allowable as indicated above (note that claims 58-61 depend from claim 29)

f) The Examiner Appears to Have Misread Bender.

In the Office Action, the Examiner pointed out that Bender distinguishes steganography from encryption. (Office Action, p. 5). The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a message into the underlying data without changing its perceptible characteristics (i.e., "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

Examiner's comments regarding Bender and certain other references suggest that the Examiner has misinterpreted the references. For example, Examiner states several times that "Bender et al. teaches encrypting digital watermarks into information with a key." (See ¶¶ 18, 19, 20, 21, 22 and 23 of the Office Action).

This assertion is inaccurate. It may be fair to characterize Bender to teach encoding watermarks into information, but Bender does not teach "encrypting watermarks into information"—much less "encrypting watermarks into information with a key." Because the Examiner's phraseology is also inconsistent with the language of Bender, it is not entirely clear how the Examiner is construing Bender, especially since the Examiner fails to relate the techniques taught by Bender to the step of "encrypting watermarks into information with a key."

g) The Combination of Bender and Barton Does Not Disclose the Claimed Inventions.

Examiner rejects claims 26, 30, 52-54, and 55-57 as unpatentable over Bender in view of Barton. (See ¶¶18 and 26 of the Office Action).

In addition to the other reasons identified, Claims 52-57 are allowable for the reason that the combination of Bender and Barton fail to yield another aspect of claim 52. Claim 52 relates to "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream." Implicit in Claim 52 is that multiple watermarks exist in the same sample stream. The Examiner has not established where Bender (or even Barton) teaches the use of multiple watermarks. Unless you have multiple watermarks, there is no need to consider marking them with unique data.

The section of Barton cited by Examiner does not make obvious claims 52-55 for at least the additional reason that Barton fails to disclose "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream":

> The invention provides a method and apparatus for basic authentication of a digital block and for carrying additional authentication information provided by the user, i.e. meta-data, in a secure and reliable fashion. To embed authentication data into a digital block, a digital signature is formed that is a reduced representation of the digital block. The signature and additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance authentication capability. The encrypted data can be further verified using error correction coding techniques. For sequential data, such as the frames of a video display, a sequence numbers can also be provided as part of the meta-data to ensure that frames have not been deleted or re-ordered.

(U.S. Patent No. 5,912,972, Col. 4, lines 18-33). As understood, Barton encodes authentication information into a digital block by first making a digital signature of the digital block, adding meta-data provided by the user, and then encoding the digital signature and the meta data into the digital block. Barton further suggests that where the underlying data comprises sequential data such as video frames (for example, where the digital blocks represent video frames), the meta data being added can include frame numbers to indicate the sequence order. It would appear that the Examiner's argument has assumed that the meta-data represents a watermark (because it represents independent data provided by the user). The Examiner, however, is relying on the insertion of sequence information that directly relates to the underlying data. Thus, at best the Examiner's citation of Barton suggests that unique information about the underlying data can be added to the meta data to provide information about the underlying data. Claim 52 is directed to the unique identification of multiple watermarks that may be embedded into underlying data. Barton, at best, appears to teach the unique identification of the underlying data. The motivation for marking Barton's underlying data is based upon the purpose of the underlying data (e.g., video frames). This motivation does not suggest any need or desire to uniquely mark the data that is being embedded into the underlying data. So, even if you assume a motivation for combining Barton and Bender, you still do not have the invention of Claim 52, and therefore claim 52, and claims 53-57 that depend from claim 52, are not obvious. The rejection must be withdrawn.

Regardless, claims 26, 30, 52-54, and 55-57 are dependent on independent claim 25. For at least the reasons discussed above in connection with the patentability of claim 25, claims 26, 30, and 52-57 are patentable. MPEP 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.") (quoting In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)). Applicant respectfully requests that the Examiner withdraw the rejection of all claims dependent therefrom.

h) The Combination of Bender and Braudaway Does Not Disclose the Claimed Inventions.

Examiner rejects claims 38 and 39 as unpatentable over Bender in view of Braudaway. (See ¶22 of the Office Action). In addition to the reasons stated above, Applicant submits that this rejection is improper because the combination of Bender and Braudaway does not yield the claimed invention.

The Examiner has failed to establish a prima facie case of obviousness to support the rejection of claims 38 and 39. The examiner asserts that in "the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of the watermark."[6] From this mere assertion, the Examiner concludes, "This change in brightness anticipates claims 38's spectral values." (Office Action, p.11). This conclusion is completely unsupported by any reasoning. The Examiner has not identified any portion of Braudaway that discloses "decoding a single message bit from a single spectral value," and for this additional reason, the rejection is untenable.

The examiner further asserts that "in the abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark." From this assertion, the Examiner concludes, "These non-transparent values form a map to meet claim 39." This conclusion too is completely unsupported by any reasoning. Braudaway, in fact, does not reference any "map." The Examiner's logic has not been expressed, and therefore, it would appear sufficient to say that Braudaway does not disclose the step of "using a map table to define where watermark information is to be encoded based on random or pseudo-random masks into the carrier signal, wherein the map table is defined such that any index of the map table enables encoding

[6] Arguably, Braudaway is teaching visible distortions so that they can be easily seen—not hidden in plain view as required by the present invention. Such visible distortions can be modified with little or no penalty to the carrier signal

information" as required by the rejected claim. For this additional reason, the rejection must be withdrawn.

i) The Combination of Bender and Schneier Does Not Disclose the Claimed Inventions.

Examiner rejects claims 40-43 and 46-48 as unpatentable over Bender in view of Schneier. (See ¶23 of the Office Action). Examiner also rejects claims 50-51 and 58-61 as unpatentable over Bender in view of Schneier and Barton, and claims 44, 45 and 49 as unpatentable over Bender in view of Schneier and Cox. (See ¶¶24-25 of the Office Action). In addition to the reasons stated above, Applicant submits that this rejection is improper because the combination of Bender and Schneier does not yield the claimed invention.

The Examiner relies on Schneier's discussion of the Digital Encryption Standard as follows:

> Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted into the encryption of block data. The key breakdown and the subsequent permutation correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of [Applicants'] claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious . . . to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

(Office Action, pp. 11-12).

DES is an encryption standard; DES is not the same as steganographic ciphering. DES processes data without regard to the perceptibility of the data, and so, the end result is an encrypted data output that looks nothing like the input. DES does not involve hiding a watermark into independent data, but rather taking the independent data and modifying it to the point that it no longer looks resembles its initial appearance. Thus, there is no "mask set" in a DES cipher. Contrary to the Examiner's assertion, the key breakdown and permutations are simply data, and bear little relationship, if any, to the mask set claimed in the present application. Accordingly, Applicants traverse the Examiner's assertion that the "key breakdown and subsequent permutations correspond to applicant's mask set." *Id.*

Claims 40-51 rely on the use of a "mask set." Because Schneier fails to disclose or suggest the use of a mask set as disclosed in the claims (whether alone or in combination with the other references), and even fails to disclose the use of a stega-cipher, the rejections of claims 40-51 must be withdrawn.

j) § 103 Rejections Based on Rejection of Claims 33 and 34

The Examiner asserts that Claim 34 is obvious in view of Bender, yet the basis provided for this assertion does not appear to be related to Claim 34. (See ¶19 of the Office Action). Examiner asserts that "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it." (Office Action, p. 9). Claim 34 is directed, in part, to "modifying the first derivative encoded signal" that was initially referenced in Claim 33. The arguments articulated by the Examiner in ¶34 do not appear to be directed to claim 34. For this reason, Examiner has failed to establish a prima facie case of obviousness. Moreover, because Bender fails to teach or suggest "generating a first derivative encoded signal" as referenced in Claim 33 and 34, the rejection based on 103 is improper. For this additional reason, Applicant requests that the 103 rejection of claim 34 be withdrawn. Applicant also requests that the 102 rejection of claim 33 be withdrawn for the same reason.

2. There Is No Motivation To Combine References.

a) Statement of the Law

The examiner has failed to establish a prima facie case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. More particularly, there is no motivation to combine Bender with the following references: Morris; the Powell Patent (U.S. Patent No. 5,930,377)[7]; Braudaway; Schneier; and Cox.

According to the MPEP,

[7] The Examiner has used two different Powell references. In making rejections on 35 U.S.C. 102, the Examiner relies upon an article, and in making 103 rejections, the Examiner relies upon the same article for some objections, while relying on the Powell Patent for other 103 rejections. That distinction is also maintained in this response by referring to the second Powell reference as the "Powell Patent."

[i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing Ex parte Clapp, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985) (emphasis added). Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing Ex Parte Skinner, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motion to combine in Winner int'l Royalty Corp. v. Ching-Rong Wang, No. 98-1553 slip op. at 14 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach that the disclosure contain therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be 'clear and particular.'" Winner at 15 (citations omitted). Further, the "absence of such a suggestion to combine is dispositive in an obviousness determination." Gambro Lundia AB v. Baxter Healthcare Corp., 11 F.3d 1573, 1579 (Fed. Cir. 1997)..

Applicant submits that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine. Instead, it appears that the Examiner has simply identified references that allegedly disclose the elements of the claim, and has combined them. Even assuming arguendo that the references contained all elements of the claimed invention, it is still impermissible to reject a claim as being obvious simply "by locating references which describe various aspects of a patent applicant's invention without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done." Ex parte Levengood, 28 USPQ2d 1300, 1303 (Bd. Pat. App. & Inter. 1993) (emphasis added).

b) Powell Cannot Properly Be Combined with Schneier

There is no motivation to combine Powell with Schneier. The Examiner relies on Schneier's discussion of DES. As explained above, DES is an encryption standard. Powell purports to relate to data hiding (i.e., steganography) because it seeks to inconspicuously embed signature points in a digital image. Absent the hindsight gained by Applicant's invention, there

is no motivation to combine the DES of Schneier with the data hiding techniques of Powell. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques, at least as suggested by Examiner. Powell is seeking to achieve a minimally changed image, whereas DES is seeking to encrypt the image. Applying DES to Powell would logically result in an encrypted image (in contravention of the teachings of Powell). Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 40-43 and 46-48 based on the combination of Powell and Schneier must be withdrawn.

c) Powell Cannot Properly Be Combined with Barton

It is not readily apparent that there is a reasonable likelihood of success in combining the techniques of Barton with the techniques of Powell, at least as suggested by Examiner. In Powell, the pixel value (which is a luminance value) is adjusted a small positive or negative amount (preferably 2% to 10% of the initial pixel value), whereby the difference is indicative of a "1" or a "0". (Powell, page 4 lines 42-48). Hence, Powell teaches replacing a pixel value with a new value that is dependent upon the initial value (adjusted upwards or downwards 2-10%) of the pixel. The Examiner cites Barton in combination with Powell in two contexts (the use of "digital signatures," and the use of sequence data). It is not readily apparent how the "signature" of Powell or the "sequence data" of Powell could be combined with Barton, where the pixel values are adjusted only a small positive or negative amount. Absent a clear way to implement the use of the "signature" or "sequence data" of Powell, it is not clear how the combinations could be successful. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 52-57 based on the combination of Powell and Barton must be withdrawn.

Furthermore, while both Powell and Barton references a "signature," the meanings of these respective "signatures" are very different. Powell's signature is not a digital signature in a cryptographic sense, but rather is an image signature. (See Powell's background section wherein he says, "the existing digital signatures are unacceptable for use with digital images.") In accordance with Powell's own teachings, the digital signatures disclose in Barton "are unacceptable for use with digital images." Thus, there is no motivation for combining Powell and Barton.

d) Bender Cannot Properly Be Combined with Morris

There is no motivation to combine Bender with Morris. The Examiner relies on Morris to suggest that "a one bit change of the least significant bit ... can be used to carry identification codes" and, therefore, it would have been obvious "to discreetly carry the watermark information of Bender et al. in the least significant bits as taught by Morris." (Office Action, ¶ 20). Bender and Morris, however, appear to be incompatible. Bender uses spread spectrum techniques to spread data out over a frequency range. The output is a composite analog signal—not digital. There is no opportunity to insert information into the LSB of Bender's carrier signal as suggested by the Examiner. In fact, Bender teaches away from such an LSB technique because it is too easy to break. (See generally Section 3.2 of Bender, p. 170). Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claim 34 based on the combination of Bender and Morris must be withdrawn.

e) Bender Cannot Properly Be Combined with the Powell Patent

There is also no motivation to combine Bender with the Powell Patent, as the Examiner has done in order to reject Claim 37. The Powell Patent is directed to images, while Bender's spread spectrum is directed to audio. As the Examiner asserts, the Powell Patent teaches "a method of embedding [that] requires use of a map of an image to determine the places to embed the watermark." (Office Action, ¶21). Because Powell's technique is directed specifically to the use of an image, and Bender is directed specifically to spread spectrum techniques for audio, it is not readily apparent why one would want to combine these references. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claim 37 based on the combination of Bender and the Powell Patent must be withdrawn.

f) Bender Cannot Properly Be Combined with Braudaway

Similarly, there is also no motivation to combine Bender with Braudaway. Braudaway is directed to images, while Bender's spread spectrum is directed to audio. The Examiner asserts that Braudaway teaches altering the brightness of certain pixels. (Office Action, p. 11). Because Braudaway's technique is directed specifically to "Color Correct Digital Watermarking of Images" (see title of U.S. Patent No. 5,530,759), and Bender is directed specifically to spread spectrum techniques for audio, it is not readily apparent why one would want to combine these references. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 38 and 39 based on the combination of Bender and Braudaway must be withdrawn.

g) Bender Cannot Properly Be Combined with Schneier

There is also no motivation to combine Bender with Schneier. The Examiner relies on Schneier's discussion of DES. As explained above, DES is an encryption standard. Bender purports to relate to data hiding (i.e., steganography). (See the Title and Abstract to Bender). Absent the hindsight gained by Applicant's invention, there is no motivation to combine the DES of Schneier with the data hiding techniques of Bender. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques, at least as suggested by Examiner. If Bender is trying to achieve steganography, it is not readily apparent how Bender would utilize DES in a steganographic manner.[8] Applying DES to Bender would logically result in an encrypted signal (in contravention of the teachings of Bender). Moreover, using DES to create an encrypted signal is not the same as the claimed invention of using a stega-cipher to steganographically encode a watermark into a carrier signal. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 40-43 and 46-48 based on the combination of Bender and Schneier must be withdrawn.

h) Bender Cannot Properly Be Combined with Cox

[8] Note that the present application does recite that DES may be used with the present invention, but the recited example relates to the use of DES prior to encoding. Moreover, the reference to DES was in connection with emulating a random bit generator: "It is possible to use a block cipher like DES in combination with a sufficiently pseudo-random seed value to emulate a cryptographically secure random bit generator." Application at p. 18, lines 21-22.

There is also no motivation to combine Bender, Schneier and Cox. In addition to the preceding section that outlines the differences in Bender and Schneier, the further combination of Cox is equally unsupported. The Examiner's apparent sole evidence of motivation is an assertion that "it would have been obvious . . . to reap the benefits" of Cox. This statement is not "clear and particular" evidence of motivation to combine, as required by the MPEP. What benefits are lacking in Schneier that are provided by Cox? Moreover, it would appear that Schneier and Cox are teaching incompatible techniques, and so, why would one skilled in the art combine them? In the absence of motivation to make the proposed combination of references, Applicants respectfully request that the rejection of claims 44, 45, and 49 be withdrawn.

CONCLUSION

Applicant maintains that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with Applicant's representative, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

Respectfully submitted,
WILEY REIN & FIELDING LLP

Date: October 4, 2002

By: Floyd B Chapman
Floyd B. Chapman Reg. No. 40,555

WILEY REIN & FIELDING LLP
Attn: Patent Administration
1776 K Street, N.W.
Washington, D.C. 20006
Telephone: 202.719.7000
Facsimile: 202.719.7049